7

Missouri Law Enforcement's Freenet Attack Now Public Record (self.Freenet)

submitted 14 hours ago * by wormnut

I just got back from a hearing in a court case involving Freenet. With the exception of a few (3?) documents that are still sealed, the government's documentation on the attack is now public record, as is the hearing itself. The transcript has not yet been published, (it is expected to take two weeks) but I took notes.

The discussion thread from when a paper describing an earlier version of this attack leaked due to a misconfigured Sharepoint instance is here.

With that in mind, as a matter of public record, I can confirm:

- In September 2011, Special Investigator Wayne Becker with the Missouri ICAC Task Force started collecting publicly available keys of child pornography. Initially the investigation only considered top-level manifest blocks, but when they found that to be ineffective they fetched the splitfile and considered all blocks of the file. That has been expanded into an automated process which runs daily and scrapes keys from Frost child porn boards. As of the last time SI Becker checked, there are 75k manifest blocks and 170 million split keys in this database. They call these Files of Interest.
- Starting April 2012, law enforcement has been running modified Freenet nodes which connect to opennet. Initially this was anywhere from 1 to 8 nodes, they logged *all requests and inserts* they observed to CSVs, and ran through most of 2014. Those logs have been retained. This was with a patch developed by people at the University of Massachusetts Amherst.

- In winter 2014, the university researchers developed an improved version which only logs requests for blocks from Files of Interest. It can optionally, defaulting to disabled, forge DataNotFound results for FOI blocks. There are around 30 of these nodes running, and have been for two years now.
- When the attack produces results which indicate, in the police's judgement, that a node is probably requesting child pornography, they will fetch the file in question, verify its contents, and retain the file.
- Dr. Brian Levine is part of the team that developed the improved attack. He made an analogy about distributing M&Ms among a room of people that went something like:

> One person starts with a bag of 100 M&Ms, someone chooses 4 people to give them to, split roughly evenly between. Each of them do the same until each person has M&Ms. Someone receiving 25, if they know the starting M&M count and the number of people the person giving them M&Ms is splitting their M&Ms between, can evaluate the probability that the person giving M&Ms is the one holding the bag.

Here an M&M is a request for a block, and the attack allows making a prediction as to whether the node that sent a request is requesting the entire file or just relaying requests. To do this it uses knowledge of the total size of the file in question from the collection of keys, and the peer count of the peer - shared by default. ("Shall we send our peers' locations to our peers? Doing so helps routing but gives some information away to a potential attacker." under Config > Core in advanced mode.) It compares the received request count to a model which assumes uniform request distribution. They ran simulations, and claim to have established a false positive rate of 2% because they ran it against HTL 16 requests and it gave a positive result 2% of the time. (Even though an HTL 16

request indicates the node sending the request is never the originator given default settings.) I am not convinced this is a valid way to establish a false positive rate. These requests are one hop more diffuse, so they are not representative of the level of diffusion present in the actual requests they use it on. I'm not clear on the distribution of distances requests can be expected to have been probably routed for a given HTL; that would be relevant here.

- Using this technique they have performed, either with a search warrant or with consent, over 50 searches in the US and Canada.

Here's a document I used as a source for some of this: ~~Affidavit Referral Narrative~~. *EDIT: The government contacted the defense and asked that I please take down this document. I have done so. They have also asked that I not make further posts about this case until it is complete.* (Search count from page 2 #13.) I redacted the section on specifics to the case out of respect for the defendant, but the broad strokes are:

1. An "undercover *Freenet* node" routes requests from a node for blocks from an FOI, and logs them.
2. Later analysis on logged requests suggests the peer in question was the originator.
3. Through an IP geolocation check (for jurisdiction) and an ISP subpoena the police obtain a name and address.
4. Police file for a warrant, telling the judge the "number and timing of the requests was significant enough to indicate that the IP address was the apparent original requester of the file." It is my opinion that the warrant affidavit does not give enough information for a judge to independently assess the reasonability of this conclusion.
5. Knock knock.

If people care I can go through and redact the things specific to the defendant more precisely; it was easier to draw two big

rectangles. (I might also be persuaded to bother to figure out how to redact PDFs properly, but for the time being I'm trying to get this posted quickly and imagemagick is easy.)

The defense will move to unseal one of the documents. For those who have PACER access, the case number is `4:16-cr-258 CEJ (NAB)` . Also it turns out some cars' black boxes record GPS location information.

2 comments **share**

all 2 comments

sorted by: **best**

[-] **kyousaya4life** 1 point 9 hours ago

Is it still believed to have an 80+% false positive rate?

permalink **embed**

[-] **nufra** 2 points 9 hours ago

we do not know yet.

Their verification procedure for their algorithm was roughly: they searched 50 people turned up in the process and found that either

- there was child porn OR
- the owner said there might have been child porn OR
- the owner had used encryption software so police could not completely rule out that there might have been child porn.

That boils down to: "the computer they found requested child pornography because there was encryption software on it".

("in nearly ever case" ... "the user had encrypted files")

Going by this, they could even have a 96% false positive rate (if all but two only had encryption software).

permalink **embed** **parent**

π